(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
7 August 2003 (07.08.2003)

PCT

(10) International Publication Number
WO 03/065169 A2

(51) International Patent Classification[7]: G06F

(21) International Application Number: PCT/US03/02931

(22) International Filing Date: 30 January 2003 (30.01.2003)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
10/060,011 30 January 2002 (30.01.2002) US
10/060,039 30 January 2002 (30.01.2002) US

(71) Applicant *(for all designated States except US)*: **TECSEC, INC.** [US/US]; Suite 220, 1953 Gallows Road, Vienna, VA 22182 (US).

(72) Inventors; and
(75) Inventors/Applicants *(for US only)*: **SCHEIDT, Edward, M.** [US/US]; 1048 Dead Run Lane, McLean, VA 22101 (US). **DOMANGUE, Ersin** [US/US]; 7006 Woodbine Road, Woodbine, MD 21797 (US). **BUTLER, Roger** [US/US]; Centreville, VA (US). **TSANG, Wai** [US/US]; 3417 Putnam Road, Falls Church, VA 22042 (US).

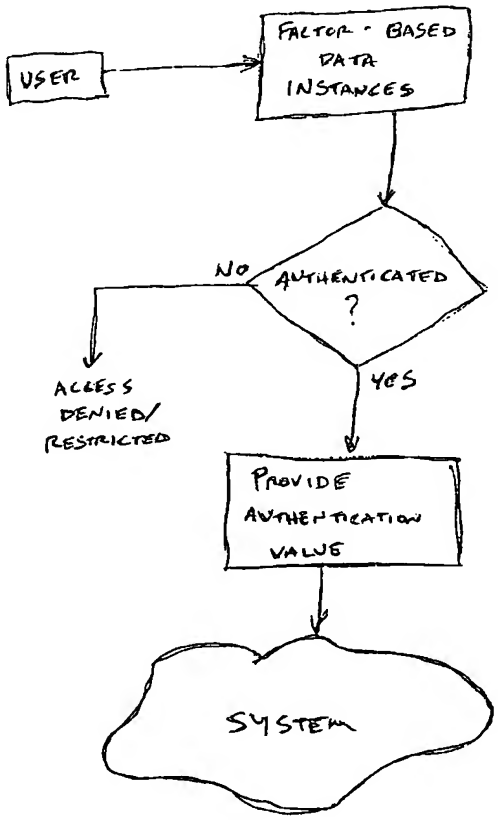
(74) Agent: **CHAMPAGNE, Thomas, M.**; IP Strategies, P.C., Suite 301, 806 7th Street, N.W., Washington, DC 20001 (US).

(81) Designated States *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, OM, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM),

[Continued on next page]

(54) Title: ACCESS SYSTEM UTILIZING MULTIPLE FACTOR IDENTIFICATION AND AUTHENTICATION



(57) Abstract: A method of securing an object at an access level includes selecting a profile for a user, including a credential having an encrypted credential public key, an encrypted credential public key encryption key, and a multiple-level access identifier. A working key is generated by binding a domain value with a random value. The object is encrypted with the working key. A random value encryption key is generated based on the shared value by decrypting the credential public key encryption key with the profile key encryption key, decrypting the credential public key with the credential public key encryption key, generating an ephemeral key pair, and generating a shared value based on the ephemeral private key and the credential public key. The random value is encrypted with the random value encryption key, and the encrypted object, the ephemeral public key, and the encrypted random value are provided for an authorized recipient. Authenticating the identity of a user to determine authorization for access to the system includes providing a plurality of factor-based data instances corresponding to a user, evaluating the factor-based data instances to determine if the user's identity is authenticated, and granting or restricting the user's access to the system if the user's identity is authenticated.

WO 03/065169 A2